REMARKS

Claim 1 has been amended to incorporate features of Claims 2 and 9, which accordingly have been canceled without prejudice. Claims 3, 4, 6, 7, 10-16 have been amended to depend from Claim 1 and/or for consistency with the amendment of Claim 1. Claim 5 has been canceled without prejudice.

Claim 24 has been amended. Support for the amendment of Claim 24 appears in the specification at least at page 17, lines 18-24.

The headings below are numbered to correspond with the heading numbering used by the Examiner in the Office Action.

Request for Examiner Interview.

Should the Examiner be of the opinion that this Amendment does not place the application in a condition for allowance, Applicant respectfully requests an Examiner Interview prior to the issuance of the next communication from the USPTO to expedite prosecution.

5. Claims 1, 3-4, 7-8, 14, 18, 20 satisfy 35 U.S.C. § 101.

The Examiner states:

> The "determining whether said call … " per se does not produce a tangible result. (Office Action, page 2.)

To expedite prosecution, Claim 1 has been amended to incorporate features of Claim 9 and now recites:

> A method comprising:
> stalling a call to a critical operating system (OS) function; and
> determining whether said call is from execution of a return instruction comprising:
> looking up a value at a previous top of stack; and
> determining whether said value is equivalent to an address of said critical OS function,
> wherein upon a determination that said call is from execution of said return instruction during said determining, **said method further comprising taking**

GUNNISON, McKAY & HODGSON, L.L.P.
Garden West Office Plaza
1900 Garden Road, Suite 220
Monterey, CA 93940
(831) 655-0880
Fax (831) 655-0888

protective action to protect a computer system. (Emphasis added.)

Accordingly, Claim 1 satisfies 35 U.S.C. § 101. Claims 3-4, 7-8, 14, 18, 20, which depend from Claim 1, satisfy 35 U.S.C. § 101 for at least the same reasons as Claim 1.

For the above reasons, Applicant respectfully requests reconsideration and withdrawal of this rejection.

6. Claim 24 satisfies 35 U.S.C. § 101.

The Examiner states:

> The phrase "A computer program product comprising" is not necessarily embodied software on computer readable media (subject to inclusion of said subject matter in the specification) corresponding to a method of said embodied software. (Office Action, page 2.)

To expedite prosecution, Claim 24 has been amended and now recites:

> A computer program product **comprising a tangible computer readable medium containing computer program code** comprising:
> a Return-to-LIBC attack blocking application for stalling a call to a critical operating system (OS) function;
> said Return-to-LIBC attack blocking application further for looking up a value at a previous top of stack; and
> said Return-to-LIBC attack blocking application further for determining whether said value is equivalent to an address of said critical OS function, wherein upon a determination that said value is equivalent to said address of said critical OS function, said Return-to-LIBC attack blocking application further for taking protective action to protect a computer system comprising said Return-to-LIBC attack blocking application. (Emphasis added.)

Accordingly, Claim 24 satisfies 35 U.S.C. § 101.

GUNNISON, McKAY & HODGSON, L.L.P.
Garden West Office Plaza
1900 Garden Road, Suite 220
Monterey, CA 93940
(831) 655-0880
Fax (831) 655-0888

For the above reasons, Applicant respectfully requests reconsideration and withdrawal of this rejection.

7-31) Claims 1, 3-4, 6-8, 10-24 are novel over Baratloo.

Claim 1 has been amended to incorporate features of Claim 2. Accordingly, the rejection of Claim 2 shall be discussed as applied to amended Claim 1.

The Examiner states:

> Claim 2 ***additionally recites*** the limitation that; "The method of Claim 1 wherein said determining whether said call is from a return instruction comprises:
> **looking up a value at a previous top of stack;** and\
> **determining whether said value is equivalent to an address of said critical OS function.".**
>
> The teachings of Baratloo are directed towards said limitations (i.e., Sections 4-8 generally, and more particularly sections 6-8, whereas the libverify '**return address verification scheme** ..." technique with the associated system call/return (i.e., OS call stalling) interceptor called as part of the operating system kernel, and associated modification and retention of user code size, location, addressing structures such that the Intel IA32 Processors process stack architecture is used, and therefore clearly encompasses the claimed limitations as broadly interpreted by the Examiner. (Office Action, pages 3-4, emphasis added.)

The Examiner's statement is respectfully traversed. Baratloo teaches that the return address is saved at the start of a function as a canary value and **the return address is compared to the canary value** at the end of the function to determine whether the return address was modified during execution of the function. If the canary value does not match the return address, **the return instruction is not executed.**

Specifically, Baratloo teaches:

GUNNISON, McKAY & HODGSON, L.L.P.
Garden West Office Plaza
1900 Garden Road, Suite 220
Monterey, CA 93940
(831) 655-0880
Fax (831) 655-0888

> Both methods **protect return addresses** on the process stack by **saving canary values at the start of a function** and **verifying the canary value at the end of the function** to determine if any buffer overflow occurred. … The wrapper_entry function **saves a copy of the canary value** on a canary stack and then jumps to the copied function. The wrapper_exit function **verifies the current canary value** with the canary stack. … **If the canary value is not found on the canary stack, then the function determines that a buffer overflow has occurred.** In that case, the wrapper_exit function then calls the die() function, which creates a syslog entry, prints an error message to the standard error device, and **terminates.** … libverify **uses the actual return address as the canary value** for each function. (Section 6, emphasis added).

Accordingly, Baratloo teaches the return address is compared to the canary value, which was the return address at the start of the function. The Examiner has failed to callout where Baratloo teaches or suggests "**looking up a value at a previous top of stack**; and **determining whether said value is equivalent to an address of said critical OS function**" as recited in amended Claim 1, emphasis added.

Further, Baratloo teaches that the return address verification is performed **before the return instruction is executed**. If the return address is not verified, **the return instruction is not executed**. Specifically, Baratloo teaches:

> … control flow is still protected because the actual value of any return address is explicitly verified **before execution of that return instruction**. (Section 6, emphasis added.)

Accordingly, Baratloo teaches that the verification is performed prior to execution of the return instruction.

First, as the verification is performed prior to execution of the return instruction, Baratloo necessarily does not teach "determining whether said call is **from execution of a return instruction**" as recited in amended Claim 1, emphasis added.

GUNNISON, McKAY & HODGSON, L.L.P.
Garden West Office Plaza
1900 Garden Road, Suite 220
Monterey, CA 93940
(831) 655-0880
Fax (831) 655-0888

Second, just prior to execution of the return instruction, the stack pointer (top of the stack) points to the return address being verified, which will be popped from the stack if the return instruction is executed. Accordingly, Baratloo does not teach "looking up a value **at a previous top of stack**" as recited in amended Claim 1, emphasis added.

As set forth in MPEP § 2131, Eighth edition, Rev. 5, August 2006 at page 2100-67:

> A claim is anticipated **only if each and every element** as set forth in the claim is found, either expressly or inherently described, in a single prior art reference. (Emphasis added.)

As Baratloo fails to teach each and every element of Claim 1, Claim 1 is allowable over Baratloo. Claims 3-4, 6-8, 10-21, which depend from Claim 1, are allowable for at least the same reasons as Claim 1.

Claims 22, 24 are allowable for reasons similar to Claim 1. Claim 23, which depends from Claim 22, is allowable for at least the same reason as Claim 22.

For the above reasons, Applicant(s) respectfully request reconsideration and withdrawal of this rejection.

Conclusion.

Claims 1, 3-4, 6-8, 10-24 are pending in the application. For the foregoing reasons, Applicant respectfully requests allowance of all pending claims. If the Examiner has any questions relating to the above, the Examiner is respectfully

GUNNISON, McKAY & HODGSON, L.L.P.
Garden West Office Plaza
1900 Garden Road, Suite 220
Monterey, CA 93940
(831) 655-0880
Fax (831) 655-0888

requested to telephone the undersigned Attorney for Applicant(s).

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on May 16, 2007.

Attorney for Applicant(s)

May 16, 2007
Date of Signature

Respectfully submitted,

Serge J. Hodgson
Attorney for Applicant(s)
Reg. No. 40,017
Tel.: (831) 655-0880

GUNNISON, McKAY & HODGSON, L.L.P.
Garden West Office Plaza
1900 Garden Road, Suite 220
Monterey, CA 93940
(831) 655-0880
Fax (831) 655-0888